REMARKS/ARGUMENTS

1. **Summary of the Office Action**

Claims 1-2, 12, 14, 20, 21 and 28 stand rejected under 35 U.S.C. 102(b) as allegedly being anticipated by Lei Tang (Method for Encrypting and Decrypting MPEG Video Data Efficiently) recited in the IDS, paper number 4 by Applicant. Claims 3-6, 13, 15-17, 19, 22-23 and 25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Lei Tang (Method for Encrypting and Decrypting MPEG Video Data Efficiently) recited in the IDS, paper number 4 by Applicant, in view of Rhoads (6,567,533 B1).

2. **Claim Objections**

Reference signs and parentheses have been removed from all claims to meet the objection contained in section 3 of the Office Action.

3. **Response to § 112 Rejections**

In response to the objections to claim 31, this claim has been amended. The technical designation of the subject matter has been amended to a 'System for distribution of information,' to reflect the fact that the claim limitations are apparatus features rather than activities. Furthermore, the phrase 'for example' has been removed. Claims 32 and 33 (newly filed) define the examples previously referred to in claim 31. Claims 15 and 16 have also been amended and it is submitted that the antecedent basis in these claims is correct.

3. Response to § 102 Rejections and § 103 Rejections

Claim 1

Novelty

Claim 1 is novel over Tang, L., 'Methods for Encrypting and Decrypting MPEG Video Data Efficiently', *Proceedings of ACM Multimedia 96*, Boston, Nov., 18-22, pp. 219-229, hereinafter referred to as D1.

D1 does not disclose means for scrambling the information signal in dependence of the entropy distribution to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal. Instead, although DCT coefficients of the information signal are determined, a permutation list is used as a secret key to map a block of DCT coefficients to a vector (page 223, right-hand column, second paragraph). Thus, no entropy information is used as input to the scrambling process, so that the scrambling is not 'in dependence on the entropy distribution'. Furthermore, it is observed that the information signal has a different entropy distribution from the entropy distribution of the signal comprising the DCT coefficients. Thus, the scrambled information signal resulting from the mapping hasn't an entropy distribution corresponding with the entropy distribution of the information signal (i.e. the signal on which the entropy distribution analysis is carried out). Thus, claim 1 is novel over D1.

Claim 1 is also novel over US-B1-6 567 533. It is assumed, but not conceded that US-B1-6 567 533 is entitled to the effective date of U.S. application 09/186,962, of which it is stated to be a continuation. However, US-B1-6 567 533 does not disclose means for scrambling the information signal. Instead, it discloses that a scaled noise signal sample is added to an input signal sample, to effect a modulation of the input signal that is generally imperceptible

(column 17, lines 9-16). Thus, the subject matter of claim 1 is novel compared to US-B1-6 567 533.

Obviousness

The subject matter of claim 1 is not obviously suggested or disclosed by a combination of D1 and US-B1-6 567 533 either.

D1 concerns the incorporation of cryptographic techniques with digital image processing technology (abstract), and is thus considered to be the more closely related to the invention than US-B1-6 567 533. The latter document does not concern scrambling of information signals, but only watermarking, in order to trace information signals.

Claim 1 differs from D1 in that D1 does not disclose means for scrambling the information signal in dependence on the entropy distribution of the information signal to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal. Instead, D1 only discloses Huffman encoding, i.e. *compression* in dependence on the entropy distribution of a signal.

The effect of this difference is that it is possible to use existing compression techniques on a scrambled information signal, thus limiting the bandwidth needed to transmit the scrambled information signal, whilst at the same time keeping the information signal secure. In contrast, the method disclosed in D1 is either more easily breakable or requires more transmission capacity. In the variant wherein the DCT coefficients are only permuted, the key can be guessed, because the largest values correspond to the lower order DCT coefficients. Where the DCT values are first 'split' (page 224, left-hand column), the entropy of the scrambled signal is higher. Thus, the attainable amount of compression is lower.

The solution to the problem of providing a more secure and efficient manner of distribution of a compressed and scrambled information signal is not to be found in US-B1-6 567 533. Firstly, the skilled person seeking to improve the method of D1 by removal of

the drawbacks noted above would not consult US-B1-6 567 533, as it concerns a different topic, namely watermarking, as opposed to scrambling. Secondly, even were one to consult US-B1-6 567 533, one would not arrive at a system falling within the scope of claim 1, because US-B1-6 567 533 does not disclose means for scrambling the information signal in dependence of its entropy distribution. Rather, US-B1-6 567 533 discloses that noise is added to or subtracted from the information signal in dependence on a code word (column 17, lines 14-15).

As D1 does not disclose using the entropy distribution for any other purpose than Huffman coding, D1 could be said to point away from the present invention, which is, accordingly not obvious in light of the cited art.

Claims 2-11

Claims 2-11 define systems comprising all the features of claim 1. For this reason, the subject matters of these dependent claims are also novel and non-obvious.

Claim 12

Novelty

Claim 12 is novel over D1, because D1 does not disclose means for scrambling the information signal in dependence on the entropy distribution of the information signal to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal (see reasoning above with respect to claim 1). Thus, claim 1 is novel over D1.

Claim 12 is also novel over US-B1-6 567 533, because that publication does not disclose means for scrambling the information signal (see above in relation to claim 1).

Obviousness

The subject matter of claim 12 is not obviously suggested or disclosed by a combination of D1 and US-B1-6 567 533 either.

D1 concerns the incorporation of cryptographic techniques with digital image processing technology (abstract), and is thus considered to be the more closely related to the invention than US-B1-6 567 533. The latter document does not concern scrambling of information signals, but only watermarking, in order to trace information signals.

Claim 1 differs from D1 in that D1 does not disclose means for scrambling the information signal in dependence on the entropy distribution of the information signal to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal. Instead, D1 only discloses Huffman encoding, i.e. *compression* in dependence on the entropy distribution of a signal. Thus, the subject matter of claim 12 differs from D1 in the same manner as the subject matter of claim 1, and is therefore not obviously suggested or disclosed by the combination of D1 and US-B1-6 567 533 for the same reason.

Claim 13, 26, 28 and 29

Claims 13, 26 and 28 define systems for scrambling an information signal having all the technical features of the system according to claim 12. Thus, the subject matters of these claims are also novel and non-obvious.

Claim 14

Novelty

Claim 14 is novel over D1, because D1 does not disclose means for combining the descrambling and scrambled information signals to obtain the information signal. Instead, D1 discloses that the decoder permutes DCT coefficients (which make up the scrambled information

signal) to their original position (page 224, left-hand column, last-but one paragraph). Thus, even were one to erroneously regard the permutation list as a 'descrambling signal', it is not *combined with* the scrambled information signal.

It is observed that the passage relied on in the Office Action to establish a case of lack of novelty relates to a related technique, not incorporated into the method that is the subject of D1. Thus, it is to be treated as a separate disclosure that cannot be combined to establish a case of lack of novelty. Furthermore, the method of selective encryption described in section 3 of D1 does not involve combining the descrambling and scrambling information signal to obtain the information signal. Instead, it involves combining a descrambled scrambled part of the information signal (the I-frames after descrambling) with an unscrambled (i.e. clear) part of the information signal (the P- and B-frames).

Claim 14 is also novel over US-B1-6 567 533, because that publication does not disclose means for descrambling a scrambled information signal to provide the information signal. Instead, it discloses a decoding process to detect embedded identification coding (column 18, lines 48-50). Thus, the known decoding process is not used to provide the information signal. For this reason claim 14 is novel over US-B1-6 567 533.

Obviousness

The subject matter of claim 14 is also not obviously suggested or disclosed by a combination of D1 and US-B1-6 567 533.

Of the two publications, D1 is considered to be more relevant to assessing obviousness. D1 relates to the combined use of image decompression and decryption, in order to provide multimedia security (see abstract). By contrast, US-B1-6 567 533 discloses techniques for watermarking content independently of whether the content is scrambled or not.

Claim 14 differs from D1 in that D1 does not disclose descrambling means that comprise means for combining the descrambling and scrambled information signals to obtain the information signal. Instead, D1 discloses permuting DCT coefficients derived from the

information signal in accordance with a permutation list (page 224, left-hand column, last paragraph). Thus, the descrambling and scrambled information signals are not combined, and the result of the 'descrambling' is not the information signal but a representation of the information signal in terms of its DCT coefficients.

The effect of this difference is that use of the known system is less secure, because the same or only a limited number of permutation lists is used to permute the DCT coefficients. Because it is known that the lower order DCT coefficients generally have higher values, the permutation list or lists can be derived from the scrambled information signal through analysis of the scrambled information signal. By contrast, the use of descrambling means comprising means for regenerating the scrambling signal as a descrambling signal and means for combining the descrambled and scrambled information signals allows for the use of what is effectively a very long key.

Thus, the invention according to claim 14 solves the problem of providing a more secure system for descrambling a scrambled information signal.

Starting from D1, the skilled person would not turn to US-B1-6 567 533 for the solution of this problem, because that publication relates to watermarking and the detection of watermarks. Even were he to do so, he would not find a disclosure of descrambling means comprising means for combining the descrambling and scrambled information signals to obtain the information signal.

For this reason, it is submitted that claim 14 is not obvious in the light of D1 and US-B1-6 567 533, and is therefore allowable.

Claims 15-25, 27, and 30

These claims relate to systems comprising all the features of a system according to claim 14. For this reason, it is submitted that they are also allowable.

Claims 31-33

Claims 31-33 define a system comprising a system according to claim 12. It is submitted that these claims are allowable because the subject matters of claims 12 is novel and not obvious.

Having tendered the above remarks and amended the claims as indicated herein, Applicants respectfully submit that all rejections have been addressed and that the claims are now in a condition for allowance, which is earnestly solicited.

If there are any additional charges, please charge Deposit Account No. 02-2666. If a telephone interview would in any way expedite the prosecution of the present application, the Examiner is invited to contact André Marais at (408) 947-8200 ext. 204.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 05/12/, 2004

André L. Marais
Reg. No. 48,095

12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1026
(408) 947-8200